Daniel Stadlin
Kantonsrat GLP
Weinbergstrasse 42c • 6300 Zug • 079 484 82 70 • ds@danielstadlin.ch • www.danielstadlin.ch

Kantonsratssitzung 5. Mai 2022

Daniel Stadlin
Interpellation von Daniel Stadlin vom 1. Oktober 2021 betreffend
Cybersicherheit – ist die kantonale Verwaltung genügend geschützt?

Stellungnahme zur Antwort des Regierungsrats

Vorlage 3308

Besten Dank dem Regierungsrat für die Beantwortung der Interpellation.

Eines vorweg: Obwohl der Kanton Zug in Sachen Cybersicherheit einiges tut, sind kantonale Verwaltung, Gerichte, kantonale Schulen, sowie die angeschlossenen Einwohnergemeinden und verwaltungsnahe Betriebe nicht wirklich genügend gegen Cyberattacken geschützt. Auch wenn die Antwort des Regierungsrats hauptsächlich allgemeine denn detaillierte Aussagen beinhaltet, kann diese Schlussfolgerung gezogen werden. Dies ist auch keine Überraschung, ist doch nur schon ein relativer Schutz sehr anspruchsvoll, ein totaler Schutz sowieso reine Illusion. So kann es laut Regierungsrat selbst beim Einsatz der besten und aktuellsten Sicherheitsmassnahmen vorkommen, dass ein Angriff gelingt und beispielsweise eine Schadsoftware eingeschleust werden kann.

So hat das Thema Informationssicherheit für den Regierungsrat denn auch eine hohe Priorität. Dabei richtet er sich nach den Datenschutzgesetzen und -vorgaben, dem ISO 27001-Standard und weiteren relevanten Sicherheitsstandards. Das ISO-27001-Zertifikat ist der Antwort beigelegt. Leider geht aus der Antwort des Regierungsrats nicht hervor, welchen Geltungsbereich die von ihm beauftragte ISO-Zertifizierung hat. Ebenfalls findet man in der Antwort des Regierungsrats keine Angaben über Faktoren bezüglich Dienstleistung und Organisation, Komplexität der IT-Infrastruktur, Abhängigkeit von Outsourcing und Lieferanten einschliesslich Cloud-Diensten, sowie interne wie externe Entwicklung von Informationssystemen. Betreibt der Kanton ein Cloud Competence Center mit eigener Informatikinfrastruktur im eigenen Rechencenter oder sind die Dienstleistungen an Dritte ausgelagert. Wenn ja, welches Level von Dienstleistungen werden vom Cloud Competence Center angeboten und um welche Firmen und Organisationen handelt es sich hierbei. Unterliegen diese Dienste ebenfalls dem Geltungsbereich nach ISO-27001 und sind entsprechende Lieferantenbeziehungsprozesse und Verträge vorhanden? Gibt es klar definierte, auf einer Sicherheitsrisikobeurteilung und Klassifizierung beruhende und technologisch kompetente Evaluationskriterien für ein mögliches Security Operation Center? Aufgrund der fehlenden Informationen in den Antworten muss davon ausgegangen werden, dass die Zertifizierung nicht in der benötigten Tiefe durchgeführt wurde. Das wäre aber sehr gefährlich, würde doch das ausgestellte Zertifikat eine falsche Sicherheit vermitteln. Womöglich ist es aber auch so, dass die fehlen Informationen vertraulich sind und gar nicht in die Interpellationsbeantwortung einfliessen konnten. Ich bitte den Regierungsrat, hierzu anschliessend noch ein paar Präzisierungen zu machen.

Durch Audits, die auf dem Vier-Augen-Prinzip basieren, soll mittels kompetenten Auditoren sichergestellt werden, dass möglichst keine Schwachstellen unentdeckt bleiben und dass systematische Fehler und Mängel ausgeschlossen werden können. Es ist deshalb notwendig, dass sowohl interne als auch externe Auditoren über die notwendigen Fachkompetenzen verfügen. Da stellt sich die Frage, ob diese Auditoren vom Kanton auch entsprechend überprüft werden. Weiter wäre es interessant zu wissen, wie diese Auditoren die Sicherheit der Informatikorganisation und des Rechenzentrums des

Daniel Stadlin
Kantonsrat GLP
Weinbergstrasse 42c • 6300 Zug • 079 484 82 70 • ds@danielstadlin.ch • www.danielstadlin.ch

Kantons einschätzen und ob risikobasierte Gefahrenmodellierungen und Verwundbarkeitsanalysen gemacht werden.

Die kantonale IT-Sicherheitsorganisation besteht aus einem IT-Sicherheitsbeauftragten in einer 50 Prozent-Stelle, der direkt dem Leiter Amt für Information und Organisation (AIO) unterstellt ist. Auch wenn zur allfälligen Bewältigung eines Cyberangriffs auf das Nationale Zentrum für Cybersicherheit des Bundes sowie weitere externe Spezialisten zurückgegriffen werden kann, dürften diese Stellenprozente eher zu knapp bemessen sein. In Anbetracht der Wichtigkeit und Dringlichkeit einer effizienten Abwehr von Cyberattacken, müsste hier eine Aufstockung ins Auge gefasst werden.

Als eines von Extrembeispielen wird in der Antwort des Regierungsrats ein Angriff mittels einer Erpressungssoftware aufgeführt. Dazu hält er fest, dass Erfahrungsgemäss das Einfallstor für Cyber-Angriffe nicht die Technik, sondern vor allem die Schwachstelle Mensch ist. Bei der Minimierung von Cyberrisiken und Qualität der Cybersicherheit stellt sich somit die Frage, ob bei der technologischen Entwicklung von Schadsoftware eine Schulung der Mitarbeitenden alle zwei Jahre wirklich genügt oder ob diese nicht intensiviert werden müsste? Die einjährige Sensibilisierungskampagne zur besseren Erkennung gefälschter oder mit einer bösartigen Software verseuchter E-Mails hat gezeigt, dass das Verwaltungspersonal insgesamt nicht auf einem akzeptablen Niveau ist. Hier braucht es dringend mehr Sicherheitsbewusstsein und auch Sicherheitskompetenzen.

Ich komme zum Schluss: Wie bereits eingangs erwähnt, muss leider festgehalten werden, dass die kantonale Verwaltung, die Gerichte, die kantonalen Schulen, die Einwohnergemeinden sowie die verwaltungsnahen Betriebe aktuell nur ungenügend gegen Cyberattacken geschützt sind. Ich fordere den Regierungsrat auf, sein Engagement in Sachen digitale Sicherheit generell zu intensivieren und den Cyberschutz technologisch wie auch personell auszubauen. Die dazu nötigen Finanzen sind ja vorhanden.

Nochmals besten Dank für die Beantwortung der Interpellation.